

Applicant: Stein et al.
For: ADVANCED ENCRYPTION STANDARD (AES) ENGINE WITH
REAL TIME S-BOX GENERATION

5

1

1. An advanced encryption standard (AES) engine with real time S-box
generation comprising:

2

3

a Galois field multiplier system in a first mode responsive to a first data
block for generating an AES selection (S-box) function by executing the multiplicative
increase in $GF^1(2^m)$ and applying an affine over $GF(2)$ transformation to obtain a subbyte
transformation; and

6

7

a shift register system for transforming said subbyte transformation to
obtain a shift row transformation;

8

9

said Galois field multiplier system being responsive in a second mode to
said shift row transformation to obtain a mix column transformation and adding a round
key for generating in real time an advanced encryption standard cipher function of said
first data block.

10

11

12

1

1

2. The advanced encryption standard (AES) engine with real time S-box
generation of claim 1 in which said first mode includes two states for executing m-1

2

3

cycles of operation including a first state for multiplying a subbyte by one to obtain a
product and then squaring the product to obtain an intermediate result and repeating with

4

5

the intermediate result m-2 times and a second state for performing the multiply and

6

square operations one more time and transforming the final intermediate result to obtain

7 the subbyte transformation.

1

1 3. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 2 in which said Galois field multiplier system includes a Galois field
3 linear transformer for each said mode.

1

1 4. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 2 in which said Galois field multiplier system includes a Galois field
3 linear transformer for each state of said first mode and for said second mode.

1

1 5. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 2 in which said Galois field multiplier system includes a Galois field
3 linear transformer and a program circuit for reconfiguring said Galois field linear
4 transformer for each mode.

1

1 6. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 5 in which said program circuit further reconfigures said Galois field
3 linear transformer for each state in said first mode.

1

1 7. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 5 in which said program circuit configures said Galois field linear
3 transformer to perform a compound multiply-square operation in said first state.

1

1 8. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 5 in which said program circuit configures said Galois field linear
3 transformer to perform a compound multiply-square operation in said first state and a
4 compound multiply-square and affine subbyte transformation in said second state.

1

1 9. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 3 in which said Galois field linear transformer associated with said
3 second mode is configured as a multiplier in said first state and as multiply-accumulate in
4 said second state to perform a mix column transformation and add a round key for
5 generating an advanced encryption standard cipher function of said first data block.

1

1 10. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 3 in which said Galois field linear transformer associated with said
3 first state is configured as a multiplier to perform a compound multiply-square operation.

1

1 11. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 3 in which said Galois field linear transformer associated with said
3 second state is configured as a multiply-adder to perform a compound multiply-square
4 and affine subbyte transformation.

1

1 12. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 1 in which said Galois field multiplier system includes at least one
3 Galois field linear transformer and an associated polynomial multiplier.

1 13. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 1 in which said Galois field multiplier system includes a
3 reconfigurable matrix of cells.

1
1 14. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 1 further including a key generator for providing a plurality of round
3 keys.

1
1 15. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 14 in which said key generator includes a key generator circuit
3 responsive to a master key to generate said round keys.

1
1 16. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 15 in which said key generator circuit includes said Galois field
3 multiplier system in a third mode for executing a multiplicative inverse in $GF(2^m)$ and
4 applying affine over $GF(2)$ transformation to obtain said round keys.

1
1 17. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 16 in which said round key includes a plurality of subkeys.

1
1 18. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 17 in which said third mode includes two states for executing $m-1$
3 cycles of operation including a third state for multiplying a subkey by one to obtain a

4 product and then squaring the product to obtain an intermediate result and repeating with
5 the intermediate result m-2 times and a fourth state for performing the multiply and
6 square operations one more time and transforming the final infinite result to obtain the
7 subkey transformation.

1

1 19. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 18 in which said Galois field multiplier system includes a Galois field
3 transformer for each of said third and fourth states.

1

1 20. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 19 in which said Galois field linear transformer is reconfigured by
3 said program circuit for said third mode.

1

1 21. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 20 in which said program circuit for further reconfigures said Galois
3 field linear transformer for each of said third and fourth states in said third mode.

1

1 22. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 20 in which said program circuit configures said Galois field linear
3 transformer to perform a compound multiply-square operation in said third state.

1

1 23. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 20 in which said program circuit configures said Galois field linear

3 transformer to perform a compound multiply-square operation and affine subkey
4 transformation in said fourth state.

1

1 24. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 18 in which said Galois field linear transformer associated with said
3 third state mode is configured as a multiplier to perform a compound multiply-square
4 operation.

1

1 25. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 18 in which said Galois field linear transformer associated with said
3 fourth state is configured as a multiply-adder to perform a compound multiply-square and
4 affine subkey transformation.

1

1 26. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 1 in which said Galois field multiplier system includes: a polynomial
3 multiplier circuit for multiplying two polynomials with coefficients over a Galois field to
4 obtain their product; a Galois field linear transformer responsive to said polynomial
5 multiplier circuit for predicting the modulo remainder of the polynomial product for an
6 irreducible polynomial; a storage circuit for supplying to said Galois field linear transformer
7 a set of coefficients for predicting the modulo remainder for a predetermined irreducible
8 polynomial; and a Galois field adder circuit for adding said product of said multiplier circuit
9 with a third polynomial with coefficients over a Galois field for performing the compound
10 multiply and add operations in a single cycle.

1 27. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 1 in which said Galois field multiplier system includes: a polynomial
3 multiplier circuit for multiplying two polynomials with coefficients over a Galois field to
4 obtain their product; a Galois field linear transformer responsive to said polynomial
5 multiplier circuit for predicting the modulo remainder of the polynomial product for an
6 irreducible polynomial; a storage circuit for supplying to said Galois field linear transformer
7 a set of coefficients for predicting the modulo remainder for a predetermined irreducible
8 polynomial; and a Galois field adder circuit for adding said product of said multiplier circuit
9 with an additive identity polynomial for performing a Galois field multiply function of the
10 input polynomials in one cycle.

1
1 28. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 1 in which said Galois field multiplier system includes: a polynomial
3 multiplier circuit for multiplying two polynomials with coefficients over a Galois field to
4 obtain their product; a Galois field linear transformer responsive to said polynomial
5 multiplier circuit for predicting the modulo remainder of the polynomial product for an
6 irreducible polynomial; a storage circuit for supplying to said Galois field linear transformer
7 a set of coefficients for predicting the modulo remainder for a predetermined irreducible
8 polynomial; and a Galois field adder circuit for adding said product of said multiplier circuit
9 with said output of said Galois field linear transformer circuit to obtain Galois field
10 multiply-accumulate function of the input polynomials in one cycle.

1
1 29. The advanced encryption standard (AES) engine with real time S-box

2 generation of claim 1 further including a plurality of Galois field multiplier systems for
3 simultaneously processing a plurality of subbytes.

1

1 30. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 17 further including a plurality of Galois field multiplier systems for
3 simultaneously processing a plurality of subkeys.

1

1 31. The advanced encryption standard (AES) engine with real time S-box
2 generation of claim 3 in which said Galois field linear transformer has a matrix of cells
3 for immediately predicting the modulo remainder of the succession of Galois field linear
4 transforms of an irreducible Galois field polynomial to obtain the ultimate output of the
5 Galois field linear transform directly in one transform cycle.

1